

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

MAR 28 2024
Mark C. McCart, Clerk
U.S. DISTRICT COURT

In the Matter of the Search of)
 Information Associated with Kik Usernames: 'kyle H,')
 'kyle11559,' that are Stored at a Premises Controlled by)
 MediaLab.ai, Inc.)

Case No.

24-mj-207-JFJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A"

located in the Central District of California, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. § 2422(b)

Attempted Coercion and Enticement of a Minor

18 U.S.C. § 2252

Certain Activities Relating to Material Involving the Sexual Exploitation of Minors

The application is based on these facts:

See Affidavit of John Haning, attached hereto.

- ☒ Continued on the attached sheet.
☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

John Haning, TFO HSI

Printed name and title

Subscribed and sworn to by phone.

Date:

3/28/24

Judge's signature

City and state: Tulsa, Oklahoma

Susan Huntsman, U.S. Magistrate Judge

Printed name and title

Jodi Jayne

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

**In the Matter of the Search of
Information Associated with Kik
Usernames: 'kyle H,' 'kyle11559,'
That are Stored at a Premises
Controlled by MediaLab.ai, Inc.**

Case No. _____

Affidavit in Support of an Application for a Search Warrant

I, John Haning, being duly sworn, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant for information associated with Kik usernames **'kyle H,' 'kyle11559,'** that are stored at premises owned, maintained, controlled, or operated by MediaLab.ai, Inc., a holding company of consumer internet brands, offering messaging applications, online education platform, and various applications for users headquartered in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require MediaLab.ai, Inc. to disclose to the government records and other information in its possession, pertaining to the individuals associated with **Kik usernames 'kyle H,' 'kyle11559,'** (hereinafter the **"SUBJECT ACCOUNTS"**).

2. I have been employed with the Rogers County Sheriff's Office for nine years. Currently, I am Lieutenant and supervisor over the Rogers County Sheriff's Office Criminal Investigations Division. I am a task force officer (TFO) with the Homeland Security Investigations (HSI), a task force officer with the FBI Safe Trails and a task force officer with the Internet Crimes against Children with the Oklahoma State Bureau of Investigations. I am a federal law enforcement officer as defined under Rule 41 and an investigative or law enforcement officer of the United States within the meaning defined in 18 U.S.C. §115(c)(1), in that I am an agent of the United States authorized by law to conduct investigations of, and make arrests for, federal offenses.

3. I am currently assigned to investigate crimes involving children. During my employment by Rogers County, I have investigated federal criminal violations related to child exploitation and child pornography. I have gained experience through training at the Internet Crimes Against Children annual conferences. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have received focused child exploitation training covering topics such as: interview techniques, live streaming investigations, undercover investigations, capturing digital evidence, transnational child sex offenders, and mobile messaging platforms utilized by these types of offenders. Moreover, I have federal authority to enforce all federal violations except immigration. I have an associate degree in criminal justice, a bachelor's in

criminal justice administration and a master's degree in criminal justice. Currently, I am completing my first year to obtain my doctorate in forensic science.

4. The facts set forth in this affidavit are based on my personal observations and information provided to me by other law enforcement officers and individuals. Because I submit this affidavit for the limited purpose of showing probable cause, I have not included each fact that I have learned in this investigation. Rather, I have set forth only facts sufficient to establish probable cause to issue the requested warrant and I have not set forth all my knowledge about this matter. Additionally, unless indicated otherwise, all statements and conversations described herein are related in substance and in part only, rather than verbatim.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 2252 (Certain Activities Relating to Material Involving the Sexual Exploitation of Children), and Title 18, United States Code, Section 2242(b) (Coercion and Enticement of a Minor) have been committed by the individuals associated with the **SUBJECT ACCOUNTS**. There is also probable cause to search the information described in Attachment A for evidence of this crime and contraband or fruits of this crime as described in Attachment B.

Jurisdiction

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. §2711(3)(A)(i).

Probable Cause

7. On March 10, 2024, Rogers County Deputy Danielle Hamilton, through her undercover profile (UCP), on the KIK Live App, began corresponding with an individual know as Kyle H. The KIK Live App is a free messaging application that uses WIFI or cellular service to communicate with others, either directly or in chat groups. In addition to its messaging capability, KIK Live allows users to join chat groups and can match users using specific criteria. Deputy Hamilton's KIK Live undercover account identifies her as a fifteen-year-old girl and the profile picture is an aged-regressed photo of Deputy Hamilton. Kyle H. told UCP he was a 26-year-old male who smoked fire (also known as methamphetamine). Kyle H. talked to UCP about smoking methamphetamine together and asked for photos of UCP. Kyle H. asked UCP if she would be willing to do anything for payment for the methamphetamine besides cash. When UCP asked what he was thinking, Kyle H. stated a hand-job. UCP stated a "blowjob" then Kyle H. said he wanted UCP to "suck it" (referring to his penis) and he asked for a picture of UCP's "butt." UCP 18 asked Kyle H. to bring her a pipe to smoke the methamphetamine and Kyle H. agreed that he would. Kyle H. sent UCP a picture of what he looked like and asked UCP if she could "deep throat" and if she would be his girlfriend. Kyle H. asked if he could give her "anal" and "cum" inside her. UCP had Kyle H. promise that he would bring her methamphetamine in return for sex or sexual favors. Kyle H. told UCP that he would bring her extra meth if she would send him a picture of her butt. Kyle said he has a

huge penis and that it would “rip [UCP’s] butt hole.” Kyle H. then repeated that UCP could be his girlfriend. Kyle H. gave UCP his phone number to text back so that they could talk outside of the KIK L App. Kyle H. sent two pictures of his fully erect penis to UCP and he told her how big he is.

8. On March 11, 2024, at around 3:18 pm, Kyle H. texted UCP and told her he wanted to meet her that day because he was needing to “nut.” He told UCP that if she were to “blow” him he would get her some meth in Catoosa. Kyle H. said she would have to give him a “blow job” in the truck while they were driving to pick up the meth. UCP told Kyle H. to meet her at the Taco Bell in Catoosa. Kyle H. said he would be on his way and he would tell her when he was there.

9. Rogers County Investigators identified Kyle H. through the picture he sent UCP and through the phone number used to text UCP. Kyle H. was identified as Kyle Jackson FUGATE.

10. When FUGATE arrived at the Catoosa Taco Bell, Deputies saw him inside of a blue GMC pickup truck. FUGATE left the Taco Bell and a traffic stop was conducted as FUGATE traveled northbound on 193rd East Avenue, Catoosa, 18 Oklahoma.

11. FUGATE was taken into custody and read his Miranda Rights. During his interview with law enforcement, FUGATE said he attended college at Oklahoma State University in Stillwater, Oklahoma. Initially, he said he was not in the area to meet anyone and that he was in the area to get a trailer to do a skid steer job. After being confronted with some of the evidence in the case, FUGATE admitted he was at

the Taco Bell to meet a girl. FUGATE admitted he communicated with the female through the Kick Live App. FUGATE said he thought he was meeting with a fifteen- or sixteen-year-old female at Taco Bell and his intention was to have sex with her. He admitted he deleted the KIK app from his phone when law enforcement pulled him over.

Background on Kik and MediaLab.ai, Inc.

12. Kik is owned and operated by MediaLab.ai, Inc., a holding company of consumer internet brands, offering messaging applications, online education platform, and various applications for users headquartered in Santa Monica, California. Kik advertises itself as “the first smartphone messenger with a built-in browser.” Kik Messenger allows users to “talk to your friends and browse and share any web site with your friends on Kik.” According to their website, Kik Messenger, a free service easily downloaded from the Internet, has become the simplest, fastest, most life-like chat experience you can get on a smartphone. Unlike other messengers, Kik usernames - not phone numbers - are the basis for Kik user accounts, so Kik users are in complete control of with whom they communicate. In addition, Kik users can exchange images, videos, sketches, stickers and even more with mobile web pages.

13. The Kik app is available for download via the App Store for most iOS devices such as iPhones and iPads and is available on the Google PlayStore for Android devices. Kik can be used on multiple mobile devices, to include cellular phones and tablets.

14. In general, providers like Kik ask their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, and other identifiers such as an e-mail address. However, Kik does not verify that information. Kik also retains certain transactional information about the creation and use of each account on their systems, including the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account.

15. Kik offers users the ability to create an identity within the app referred to as a "username." This username is unique to the account and cannot be changed. No one else can utilize the same username. A Kik user would have to create a new account in order to obtain a different username. The username for a particular Kik account holder is generally displayed in their Kik profile.

16. Given the ability for users to create multiple accounts that are not linked to a specific mobile device (i.e. a phone number), it has become a popular app used by people involved in the collection, receipt, and distribution of child pornography.

17. In my training and experience, an application user's IP log, stored electronic communications, and other data retained by the provider, can indicate who has used or controlled the application account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and

tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Kik account at a relevant time. Further, Kik account activity can show how and when the account was accessed or used. For example, as described herein, Kik logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Kik access, use, and events relating to the crime under investigation. Additionally, Kik account activity may provide relevant insight into the Kik account owner's state of mind as it relates to the offense under investigation. For example, information on the Kik account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

18. Therefore, the computers and systems of Kik, owned and operated by MediaLab.ai, Inc., are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Kik, such as account access information, transaction information, and other account information.

Characteristics Common to Individuals Who Exhibit a Sexual Interest in Children

19. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who exhibit a sexual interest in children, and who distribute, receive, possess, and/or access with intent to view child pornography:

- i. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity;
- ii. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts;
- iii. Such individuals almost always possess and maintain digital or electronic files of child pornographic material, that is, their pictures, videos, photographs, correspondence, mailing lists, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, videos, photographs, correspondence, and mailing lists for many years;
- iv. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, on their person, to enable the individual to view the child pornography images, which are valued highly. Such individuals do not

like to be away from their child pornography images for an extended period of time. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis;

- v. Based on my training and experience and speaking with other special agents, I know that such individuals have taken their electronic devices and storage media, which contain their collections of child pornography, with them when they have moved or changed residences;
- vi. Such individuals may also take it upon themselves to create their own child pornography or child erotica images, videos or other recordings, or engage in contact sex offenses with children. These images, videos or other recordings may be taken or recorded covertly, such as with a hidden camera in a bathroom, or the individual may have child victims he or she is abusing in order to produce child pornographic or child erotica images, videos or other recordings. Studies have shown there is a high cooccurrence between those who traffic in child pornography and commit sex offenses with children. Such individuals may also attempt to persuade, induce, entice, or coerce child victims in person or via communication devices to self-produce and send them child pornography or to meet in person for sex acts. These images, videos or other recordings are often collected, traded, or shared; and
- vii. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

Information to be Searched and Things to be Seized

20. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require MediaLab.ai, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information

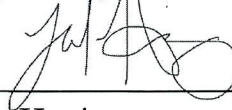
described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

Conclusion

21. Based upon the facts set forth in this affidavit, I believe that there is probable cause to believe that the location described in Attachment A contains evidence of violations of Title 18, United States Code, Section 2422 (Certain Activities Relating to Material Involving the Sexual Exploitation of Children), and Title 18, United States Code, Section 2422(b) (Coercion or Enticement of a Minor).

22. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on MediaLab.ai, Inc. Because the warrant will be served on MediaLab.ai, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully Submitted,



John Haning
Task Force Officer
Homeland Security Investigations

Subscribed and sworn by phone on March 28th, 2024



UNITED STATES MAGISTRATE JUDGE



ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the account associated with Kik usernames **‘kyle H,’ ‘kyle11559,’** (SUBJECT ACCOUNTS), that are stored at premises owned, maintained, controlled, or operated by MediaLab.ai, Inc., a company headquartered at 1222 6th Street, Santa Monica, CA 90401.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by MediaLab.ai, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of MediaLab.ai, Inc., regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to MediaLab.ai, Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), MediaLab.ai, Inc. is required to disclose the following information to the government for each account listed in Attachment A between November 16, 2023, through February 29, 2024:

- (a) All contact and personal identifying information;
- (b) All activity logs for the account and all other documents showing the user's posts and other Kik activities;
- (c) All photos and videos uploaded by the SUBJECT ACCOUNTS and all photos and videos uploaded by any user that have that user tagged in them, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;
- (d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Kik usernames; groups and networks of which the user is a member; future and past event postings; rejected "Friend"

requests; comments; gifts; pokes; tags; and information about the user's access and use of MediaLab.ai, Inc.'s applications;

- (e) All basic subscriber information,
- (f) All call detail records,
- (g) All detailed message logs,
- (h) All content, including but not limited to message content,
- (i) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that account, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
- (j) All other records and contents of communications and messages made or received by the user, including all Messenger activity, messages, chat history, video and voice calling history, and pending "Friend" requests;
- (k) All "check ins" and other location information;
- (l) All IP logs, including all records of the IP addresses that logged into the account;
- (m) All past and present lists of friends created by the account;
- (n) All records of Kik searches performed by the account;
- (o) The types of service utilized by the user;
- (p) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

- (q) All privacy settings and other account settings, including privacy settings for individual Kik posts and activities, and all records showing which Kik users have been blocked by the account;
- (r) All records pertaining to communications between MediaLab.ai, Inc. and any person regarding the user or the user's Kik account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 2252 and 18 U.S.C. § 2242(b) for the **SUBJECT ACCOUNTS**, listed on Attachment A, including:

- (a) Images of child pornography; files containing images and data of any type relating to the sexual exploitation of minors, and material related to the possession or production thereof, as defined in 18 U.S.C. § 2252;
- (b) Information, correspondence, records, documents, or other materials pertaining to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to the sexual exploitation of minors;
- (c) Communications between the SUBJECT ACCOUNTS and others pertaining to the receipt, distribution, and/or possession of child pornography from November 16, 2023, through February 29, 2024;
- (d) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

- (e) Evidence indicating the account owner's state of mind as it relates to the crime under investigation; and
- (f) The identity of the person(s) who created or used the SUBJECT ACCOUNTS, including records that help reveal the whereabouts of such person(s).